

(English version)

Question for written answer E-002186/26
to the Commission
Özlem Demirel (The Left)
(29 May 2026)

Subject: Security of Europol information systems

An internal report by Europol's Data Protection Officer, which was submitted in early 2019 and brought to light by an investigation, described significant security and data protection gaps in the CFN system ('shadow IT'), which was not subject to oversight at the time. Europol's own Data Protection Officer warned against a possible ban on the processing of the entire parallel data system, effectively amounting to a complete cessation of Europol's operational business. Since then, Europol and the European Data Protection Supervisor have been in continuous discussions on measures to address them. Last February, the Data Protection Supervisor informed the Joint Parliamentary Scrutiny Group (JPSG) that, although his inquiry had been concluded, certain issues remained unresolved, in particular in the area of IT security and the logging of data access. Of the 150 recommendations issued, fifteen had not been implemented.

1. What is the current state of security of Europol's systems, including as regards ensuring that all operations and processing steps can be properly logged, and what is the breakdown of individual access instances (including privileged access) and access rights by year, system and individual?
2. Does Europol have full control over who has access to which systems and have the deficiencies in password management been remedied?
3. How is effective oversight ensured as regards compliance with the code of conduct by all staff, posted liaison officers, and third parties with access to Europol systems?

Submitted: 29.5.2026

Answer given by Mr Brunner on behalf of the European Commission
(22 September 2026)

The security of the European Union Agency for Law Enforcement Cooperation (Europol) information systems is framed by the Europol Regulation ⁽¹⁾ and the EU data protection framework ⁽²⁾, including independent supervision by the European Data Protection Supervisor (EDPS) ⁽³⁾, with which Europol cooperates closely.

Europol is required to keep logs of its processing operations ⁽⁴⁾, which may be used to verify the lawfulness of processing, self-monitoring and ensuring data integrity and security, and are available to Europol's Data Protection Officer and the EDPS for their oversight functions. Europol is also subject to the provisions of Regulation (EU, Euratom) 2023/2841 to ensure a high level of cybersecurity ⁽⁵⁾.

Europol is required to establish the requisite security measures across its information systems to ensure a level of security appropriate to the risks ⁽⁶⁾.

The implementation of these requirements, including as regards access management, is subject to independent supervision by the EDPS.

The recent Commission proposal for a new Europol Regulation ⁽⁷⁾ includes rules on the core services and tools developed and maintained by Europol, to update its framework in response to the evolving security environment and to further strengthen the transparency and accountability of the Agency in the performance of its tasks in this new context.

The code of conduct of Europol is available on its website ⁽⁸⁾. Europol has also a dedicated Internal Investigations Service, which handles suspected misconduct, and which cooperates, where required, with the European Anti-Fraud Office, the European Public Prosecutor's Office and national competent authorities.

⁽¹⁾ Regulation (EU) 2016/794, as amended.

⁽²⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

⁽³⁾ Article 43 'Supervision by the EDPS'.

⁽⁴⁾ Article 40 'Logging'.

⁽⁵⁾ Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

⁽⁶⁾ Article 32 'Security of processing'.

⁽⁷⁾ Brussels, 24 June 2026, COM(2026) 580 final.

⁽⁸⁾ 'The Code of Conduct of Europol' is available at https://www.europol.europa.eu/cms/sites/default/files/documents/the_code_of_conduct_of_europol.pdf.